International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 4, August 2023, pp. 3631~3640
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i4.pp3631-3640

A new linear quadratic regulator model to mitigate frequency disturbances in the power system during cyber-attack

Muhammad Musleh Uddin, Kazi Rafiqul Islam, Md. Monirul Kabir
Department of Electrical and Electronic Engineering, Dhaka University of Engineering and Technology, Gazipur, Bangladesh

Article Info

Article history:

Received Jun 21, 2022
Revised Sep 7, 2022
Accepted Oct 1, 2022

Keywords:

Automatic generation control
Cyber-attack and cyber-security
Linear quadratic regulator
Load frequency control
Proportional-integral-derivative

ABSTRACT

This paper proposes a new model integrating a linear quadratic regulator (LQR) controller to mitigate frequency disturbances in the power system during cyber-attack, called as linear quadratic regulator to mitigate frequency disturbances (LQRMFD). As we know, most of the existing models have a common problem with achieving significant performances in mitigating dynamic response parameters, such as frequency deviation and settling time. However, the key aspect of LQRMFD is to mitigate the above issues with remarkable performance improvements. An uncommon and stable power system model has been considered in LQRMFD first to reach such a goal. A numerical problem has been solved to derive a certain characteristic equation, where the Routh-Hurwitz array criterion is applied for determining the stability of such a power system. After that, a state-space equation is developed from the power system to activate the LQR controller. Thus, achieving diversity and eliminating the redundancy of the power system considered can be obtained in LQRMFD. To evaluate the performance of LQRMFD, a series of experiments was conducted using the MATLAB-Simulink tool. Rigorous comparisons were also made among the results of LQRMFD, self-implemented and existing models. Furthermore, a detailed analysis was reported among those models to find the performance improvement of LQRMFD in percentage.

Corresponding Author:

Kazi Rafiqul Islam
Department of Electrical and Electronic Engineering, Dhaka University of Engineering and Technology
Gazipur, Bangladesh
Email: rafiqul@duet.ac.bd

1. INTRODUCTION

The growing electrical loads on interconnected grid systems make the system more extensive day by day. Therefore, operational deregulation causes dramatic changes in the current electrical systems. As a result, the power system (PS) becomes vulnerable and less reliable. On the other hand, providing a quality power supply has become a critical issue due to the growth of electrical loads. Considering all these aspects, in order to make the system stable, especially frequency should be kept constant to its pre-assigned value. Therefore, the whole system may collapse due to maximum frequency deviation (FD) [1].

Furthermore, high-frequency changes may cause generators to lose synchronization, resulting in terrible consequences. In the interconnected PS, the cyber threat to the power plant is considered a consequential disruption that can severely unstable the system. Advanced control measures, including the communication interface, should be taken to mitigate this disturbance. A suitable steady-state condition is required to ensure a smooth power supply.

The technological innovation of the cutting age empowers more adaptable and competent access to PS structure [2], [3]. In addition, the adverse effect of information communication technology (ICT) and digital

computer techniques (DCTs) on reliability and security is a vital issue for the management and operation of PSs. The lack of proper ICT management can increase the threat of cyber-attacks on PSs. Some sections of the power plants including advanced control loops, different sensors, and communication networks are available under ICT management. Therefore, various confidential information is transmitted through ICT, which is one of the cyber-vulnerable mechanisms of PS. At the power station, the information might be hacked when data is being sent from the detecting department to the control department. On the other hand, whenever confidential information is accessed, hacker may gain control over the automatic controller of a power plant. In this regard, any changing in the controller actions creates malicious data accessing to the controller as well as disrupting the system's stability. In addition, the reliability and security of ICT and DCTs are the vital issues for the operation of modern PSs that increasing the risk of cyber-attacks (CAs). It is noted that PS reliability is an essential aspect for measuring cyber-security threats. Therefore, such impact of threats must be assessed upon the cost of the whole PS [4].

In recent years, several cyber-attacks have been responsible for destabilizing the PS discussed in [3]–[6]. Particularly, the effect of data integrity attacks on a PS has been introduced in [3]. In [4], the impact of cyber security attacks on PS is evaluated. In contrast, the cyber security and vulnerability of the PS are also analyzed in [5], [6]. In addition, the graph technique is proposed in [7] to analyze the impact of CA on the association in between the electrical and cyber grid. Furthermore, the cyber-vulnerable components of PS and the effects of CA have been properly studied to ensure system stability mentioned in [5]–[7]. It is known that PS failure occurs due to the maximum FD. Thus, an accurate and active controller, i.e., the optimal controller, is required to maintain the desired specific frequency [8]–[10].

The recent attack on the Ukraine power grid has focused on the requirement of proper control measures to be secured power station control units [11]. The authors here analyze the Ukraine CA and propose a mitigation method. Therefore, it is required to explore the weakness of PS as well as supervisory control and data acquisition (SCADA) to avoid CAs and assess the effects of such attacks. Furthermore, the influence of CA on wind farms and PS networks is also studied in [12]. Deng *et al.* proposed a model in [13] that explores the formation of false data injection to retrieve its effect on the electricity market and to make a protection scheme against attack. A detailed discussion is available in [14] about the top twenty CAs on industrial control systems. Recently, DOS virus has been found in [2], [15], [16] to be malware that targets SCADA systems resulting in slower communication protocols as well as making the unavailability of information. On the other hand, the SCADA system has received a response from Stuxnet virus as another malware attack that is also alarming for its complexity mentioned in [15], [17].

Some works have been done in the literature to protect CA on PS (e.g., [18]–[24]). Particularly, load frequency control (LFC) and automatic generation control (AGC) units are introduced in [18]–[20] that are bound to retain stable frequency with load variation during CA. In order to overcome the effect of faulty data injection on AGC, an alternative detection technique has been proposed in [20]. Alternatively, multiple control units, that is to say, AGC-proportional–integral–derivative (PID), automatic voltage regulator (AVR), and controlled switching unit (CSU) have been introduced in [21] to ensure mitigating the voltage and frequency individually during CA, where the nominal frequency is tried to be fixed with demanding a period. After that, Mossad *et al.* proposed a method in [22] that introduces an adaptive LFC-PID controller formulated by artificial neural network (ANN) for mitigating frequency disturbances of PS during CA. Furthermore, a three-input switch for LFC of an isolated PS has been proposed in [23] to reduce FD during CA but failed to achieve PS stability because of demanding a considerable time. Islam *et al.* [24] have tried to solve the frequency disturbances problem during CA using ANN in the AGC-PID model but failed to significantly improve because of demanding larger time. Recently, Li *et al.* [25] proposed an LFC-based method for GAN networks to mitigate the frequency disturbances during CA, but no significant performance analysis has been reported. Finally, it can be concluded that, although the existing controllers (e.g., LFC, AGC, AGC-PID, 3-input switch, CSU, and ANN) tried to solve the frequency disturbances during CAs, they failed to achieve significant improvement in such cases. Therefore, an optimal and robust controller is needed to keep the desired frequency in PS.

In order to overcome the limitations mentioned above of the present solutions, a new linear quadratic regulator (LQR) model for reducing frequency disruptions in PS during CA (LQRMFD) has been proposed. The idea incorporated in this model was originally introduced in our earlier work [26]. The highlighting issue of this model is to mitigate the frequency disturbances in PS during CA with a reduced cost function. The proposed model utilizes an LQR controller in a new PS network during CA to mitigate the frequency disruptions. To facilitate such a technique, a new steady-state equation has been derived from achieving an effective and stable system model in linear quadratic regulator to mitigate frequency disturbances (LQRMFD). The reason for the novelty and distinctness of the proposed LQRMFD versus previous models (e.g. [8], [9]) lies in the following two aspects.

First, LQRMFD emphasizes not only providing the reduction of settling time (ST) but also mitigating FD of PS during CAs. LQRMFD uses an LQR controller in a particular PS network to improve the PS stability. As we know, LQR can remarkably improve the static and dynamic response of a closed-loop PS [8], [9]. Since the conventional controllers (e.g., LFC [23], integral controller, or AGC [23], AGC-PID [21], CSU [21], ANN [24]) produce a very slow dynamic response. One optimal controller (e.g., LQR) that is much more effective than conventional controllers has been invented. According to our knowledge, very few works have been done using LQR controllers for the stability of PS during CA (e.g., [27]), where they incorporate LQR control algorithms for controlling the system using PSO. This control is a full-state feedback control, where the objective function is minimized to be used in all system states.

Second, the proposed model uses a new PS network to efficiently mitigate the frequency disruption in PS during CA. It is noted that most findings in this arena were done based on similar PSs of the same ratings (e.g., [21], [23], [24]). In such cases, the potentiality of finding better problem solutions is low as the chance of diversity of PS platforms is low. On the other hand, diversity in selecting different PSs always provides an exploration of searching for better solutions. Most of the existing PSs are incorporated from [9] having similar parameter ratings, whereas our model uses a different PS with different ratings. Thus, reaching diversity as well as eliminating the redundancy of PS research can be attained in such considerations. Therefore, to achieve an effective and stable system model in LQRMFD, a new steady-state equation has been derived by solving a new numerical problem [9].

The rest of this paper is organized as follows. Section 2 describes about our proposed model LQRMFD in detail. Section 3 presents the results of our experimental studies with detailed comparisons and analysis in between the results of LQRMFD, self-implemented models and existing models. Finally, section 4 discusses the concluding remarks and future strategies.

2. THE PROPOSED MODEL LQRMFD

In this context, the proposed model, LQRMFD for mitigating frequency disturbances in PS during CA is discussed in detail. The focusing issue of this model is to provide the reduction of ST as well as mitigation of FD of PS during CAs at a time. LQRMFD incorporates an LQR controller in an uncommon PS network during CA. A new state-space equation has been derived for achieving an effective and stable system model in LQRMFD. The steps of LQRMFD can be described by the block diagram shown in Figure 1, which are described in more details as follows.

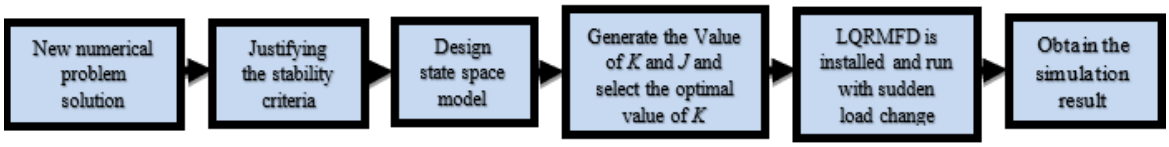

Figure 1. Block diagram of the proposed model LQRMFD

Step 1: In order to facilitate our LQRMFD perfectly, an uncommon and stable PS model has been considered here. Thus, achieving diversity as well as eliminating the redundancy of PS research can be obtained in such consideration as the common practice exists in the literature of similar PS models in most cases. Initially, an uncommon numerical problem has been considered from [9] for a single area PS in our proposed LQRMFD model. In this regard, we have solved this numerical problem according to [9].

Step 2: Justify the stability of the incorporated PS by solving this numerical problem mentioned in [9]. Precisely, a set of characteristic equations is derived from that PS model, where the Routh-Hurwitz array is applied to find the stability of the system. Determine the stable limit of R for getting stable operation of the LFC PS model. In this regard, the Routh-Hurwitz array can be used by considering the parameters mentioned in Table 1 that are summarized from [9], [26].

Step 3: Derive the steady-state equation for the LQR model in regular form from the linear model of LFC according to the steady-state variable model. After the formulation of the steady-state equations into matrix form, the values of *A*, *B*, *C*, and *D* are determined. Here, the state space equations are given in (3) to (5).

Step 4: Generate the values of *K* and *J* according to the control law and quadratic performance index procedures. Precisely, determine the optimal feedback gain K with the proper set value among the three values for a suitable transient response of the system. After that, find the value of a quadratic performance index *J* from basic LQR formulations.

Step 5: Implement our LQRMFD in MATLAB-Simulink simulator in association with the previous two steps. Prior to running LQRMFD, all parameters are required to be set by their proper values as shown in Table 1, with suddenly changing the load of 0.20 pu, which is actually the phenomenon of CA. However, after running the LQRMFD method, a FD curve is obtained for LQR power system model.

Step 6: Obtain the optimal simulation results of our LQRMFD model. According to the dynamic response parameters (i.e., FD and ST), the results are obtained optimally, which is exhibited in the part of the experimental results.

Table 1. Parameters of the proposed power system model, adapted from [9]

Symbols	Parameters	Values
τ_T	Turbine time constant	0.5 s
τ_g	Governor time constant	0.25 s
H	Generator inertia constant	8s
D	Load coefficient (1% change in frequency)	1.16
R	Speed regulation	0.04
f	Nominal frequency	50 Hz
ΔP_L	Change in load	0.25 pu
$\Delta P_L 1$	Change in load (for LQRMFD method)	0.2 pu

According to the above discussions, it is observed that the proposed LQRMFD model is very simple and easy to understand. It means that the state space equation incorporated in LQRMFD can be designed from LFC block diagram can be found [9], [26]. For more comprehensibility of the proposed LQRMFD, the following subsections are discussed to be followed.

2.1. LQR formulation

LQR controller is an optimal controller that is significant only for linear systems [8]. It is a design approach for controlling systems that involves reducing the system variable performance index. Basically, LQR uses a control method resulting in the reduction of the cost function to control the load frequency [9], [27], [28]. In LQR, weight matrices *Q* and *R* are important parameters that observe frequency changes in a single area to achieve optimal feedback improvement in the dynamic performances of LFC of a PS [8], [9]. However, the block diagram of LQR controller is presented in Figure 2.

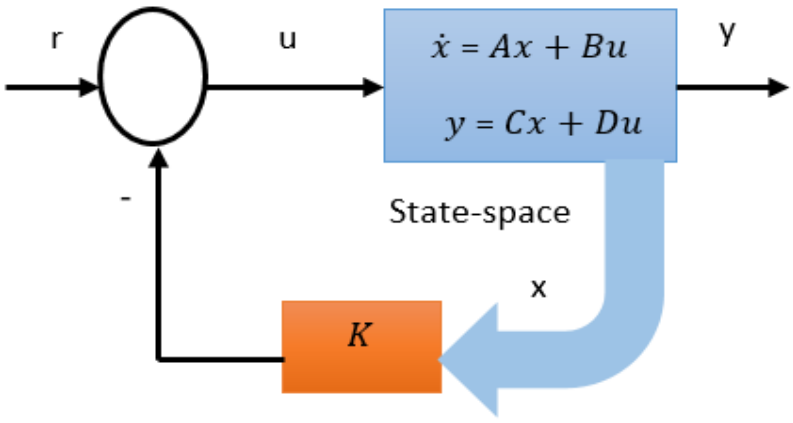

Figure 2. Block diagram of a typical LQR controller

2.2. State-space variable model

LQR gives the best performance with the given performance criteria. It is a design approach for controlling a system that reduces the system variable performance index. As we know, LQR has a remarkable ability to perform frequency controlling [8]–[10]. The state variables of the obtained control system are expressed as $x(t)$, the entrance vector of the system as $u(t)$, the exit factor of the system as $Cx(t)$, and considered $r(t)$ as zero. The state-space variable of the system is presented in (1), (2).

$$\dot{x}(t) = (t) + (t) \quad (1)$$

$$y = (t) \quad (2)$$

Here, *A*, *B*, and *C* are the state matrix, input matrix, and output matrix, respectively, among which *C* is the identity matrix and *D* is zeros. Thus, the output equation is, $Y = [0\ 0\ 1]x$. In this regard, the parameters of A, B, and C are formulated by the LFC model [9].

2.3. Obtaining control law

In LQR controller, obtaining the control law is significant for the system's accuracy. In consequence, the positive definite matrix, *P*, and the optimal feedback gain, *K*, can be obtained by applying an LQR function in the MATLAB workspace [9]. Now, to get the input of the plant, *u*(*t*) from the control law is obtained as (3).

$$u(t) = -Kx(t) = -R^{-1}B^{T}Px(t) \quad (3)$$

Here, *K* is a 1×*n* vector of constant feedback gain from which the optimal value is selected on the basis of a trial-and-error process to minimize the cost function of PS. *K* is the state feedback optimal control gain vector.

2.4. Finding the value of quadratic performance index, *J*

In LQR controller, the widely used performance index in optimal control design called as quadratic performance index, *J*, formulated by minimum error and minimum energy criteria. That's why, finding the value of *J* is a significant issue for giving the best trade-off between performance and cost of control of the PS. In our proposed method, we used the following equation to find the value of *J*, adapted from [9] as (4).

$$J = \int_0^{\alpha}(x^{T}Qx + u^{T}Ru)dt \quad (4)$$

The state space equations of LQR controller are as similar as derived in the LFC system. Now, to find the optimal feedback gain vector, minimize the performance index, *J* mentioned in [9] as (5).

$$J = \int_0^{\alpha}(40x_1^2 + 20x_2^2 + 10x_3^2 + 0.2u^2)dt \quad (5)$$

Now, according to (5), we have (6).

$$Q = \begin{vmatrix} -40 & 0 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & 10 \end{vmatrix} \quad \text{and} \quad R = 0.20 \quad (6)$$

3. RESULTS AND DISCUSSION

In this section, the performance of linear quadratic regulator to mitigate frequency disturbances (LQRMFD) to mitigate frequency disturbances in the PS during a CA was investigated. The LQRMFD performance was evaluated in terms of dynamic response parameters, such as, FD and ST. For more clarification, this context can be divided into the following subsections.

3.1. Experimental setup

In order to ascertain the effectiveness of LQRMFD for the solution of frequency disturbances during CA, extensive experiments were carried out. To reach such a goal, the MATLAB Simulink tool was considered to design the PS network using the Simulink block. In designing such a network, three steps were considered successively: i) making different connections between each block, ii) inserting required data to those blocks, and iii) finding the optimal value of feedback gain, *K*, based on trial-and-error method.

3.2. Experimental results

In the simulation results, stability performances of the proposed LQRMFD during CA were analyzed in terms of FD and ST. However, the results of our LQRMFD on the particular PS during CA are shown in Figure 3 and Table 2, respectively. It is observed that FDs were found as -0.0004 and -0.0227 in pu and Hz, respectively. On the other hand, ST for frequency stability because of CA was 0.55 sec. Thus, it can be said that the proposed model has a strong capability to make a system stable during CA.

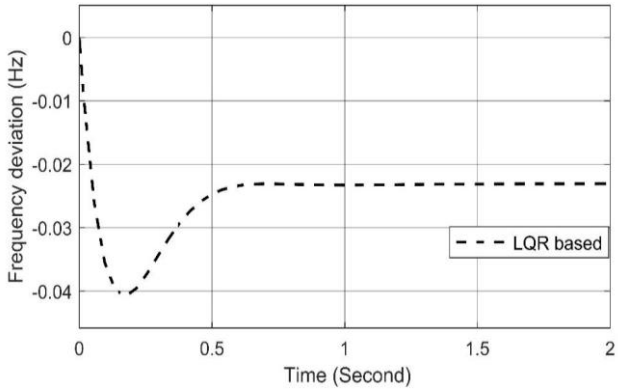

Figure 3. Frequency deviation (FD) response during cyber-attack in LQRMFD

Table 2. Results of frequency deviation (FD) response during cyber-attack in LQRMFD

Parameters	LQRMFD
FD, $\Delta\Omega$, pu	-0.0004
FD, $\Delta\Omega$, Hz	-0.0227
ST (t_s) sec	0.55

3.3. Comparisons

It has been said before that diversity in selecting different PSs always provides an exploration of better solutions. That's why, in this proposed LQRMFD, a new PS model has been incorporated by solving a new numerical problem from [9], [26]. To make a perfect comparison among the performances of our model and other existing models (e.g., LFC, AGC, and AGC-PID), it was necessary first to implement those models accordingly.

3.3.1. Comparisons with self-implemented models

In this context, the obtained results of LQRMFD were compared with the results of individual PS models with three different controllers (e.g., LFC, AGC, and AGC-PID) that were self-implemented. In this regard, the integrated PS model is similar to the incorporated one in LQRMFD. However, the experimental results obtained from the self-implemented models of LFC, AGC, and AGC-PID during CAs are exhibited in Figures 4 to 6 and Table 3, respectively. It should be noted that the block diagram and required values of the parameters of those models can be found in [9], [26].

It is observed from Table 3 that FD of the LQRMFD model is -0.0004 in pu as well as -0.0227 in Hz, which are far better than the other three models in terms of reduced quantity. On the other hand, ST for the frequency stability in the case of LQRMFD is 0.55 in second, which is a more reduced quantity compared to the other models. Thus, it can be said that our model LQRMFD has a remarkable capability to mitigate the frequency disruptions of PS during cyber-attack.

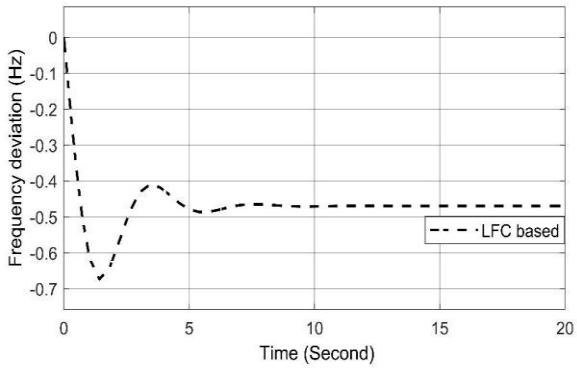

Figure 4. Frequency deviation response for LFC

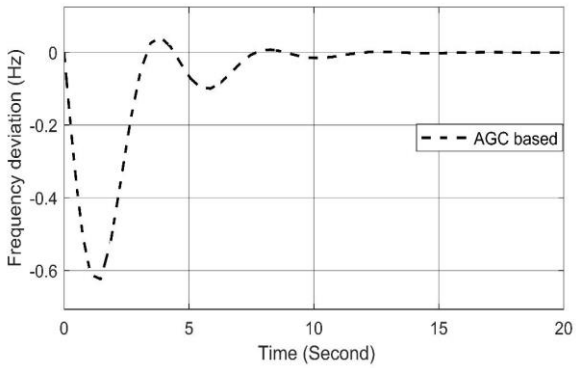

Figure 5. FD response for AGC

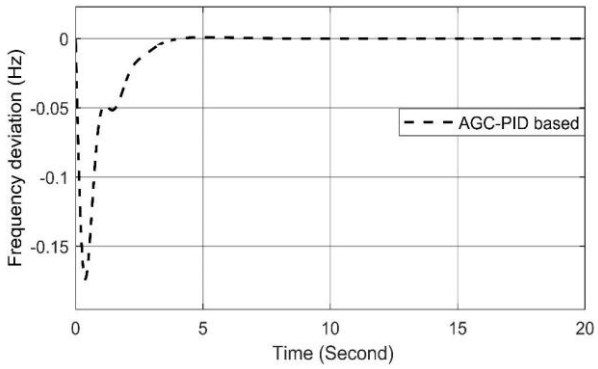

Figure 6. FD response for AGC-PID

Table 3. Comparisons among the results of self-implemented models of LQRMFD, LFC, AGC and AGC-PID using new power system as well as existing models of LFC [21], AGC [21], AGC-PID [21], CSU [21], and AGC-PID-ANN [24]. Here, "- -" refers to not available

Parameters	LQRMFD	LFC	LFC [21]	AGC	AGC [21]	AGC-PID	AGC-PID [21]	CSU [21]	AGC-PID-ANN [24]
FD ΔΩ, pu	-0.0004	- 0.0122	-0.0115	- 0.0094	-0.0072	- 0.0006	- 0.0019	0.954	- -
FD, ΔΩ, Hz	- 0.0227	- 0.6115	-0.5753	- 0.4695	- 0.3607	- 0.0318	- 0.0968	47.57	- -
ST, t_s, sec	0.55	6.70	6.90	11.00	10.95	4.70	5.85	5.08	0.76

3.3.2. Comparisons with existing models

In this context, the obtained results of LQRMFD were compared with the results of existing PS models with different controllers, such as, LFC [21], AGC [21], AGC-PID [21], CSU [21], and AGC-PID-ANN [24] mentioned in Table 3. It was observed that performance of CSU [21] was better than that of LFC-3 input switch [23]. On the other hand, it was also claimed that AGC-PID-ANN [24] had an improvement in results over the model of the LFC-3 input switch [23]. However, in this context, we used two parameters for comparisons, such as, FD and ST. The afore-mentioned five models represented a wide range of CA mitigation techniques, among which the three models, i.e., LFC, AGC, and CSU used the existing common PS platforms without incorporating any additional techniques. On the other hand, AGC-PID [21] used PID controller with AGC technique. Furthermore, ANN was integrated to be determined the optimal values of PID parameters in AGC technique in AGC-PID-ANN [24]. It should be noted that all of the afore-mentioned models adapted the common PS platforms for mitigating the frequency disturbances during CAs.

The obtained results of the existing LFC [21], AGC [21], CSU [21], AGC-PID [21], and AGC-PID-ANN [24] models are also shown in Table 3. It is observed that most of the results of those models were not presented clearly in their experimental studies except AGC-PID-ANN. They only presented ST in their experimental contexts. Therefore, it was necessary to implement those models following all the terms and conditions to summarize the experimental results in Table 3.

We can see in Table 3 that LQRMFD produced the best solutions in terms of the smallest FD during CA compared to others, that is to say, -0.0004 in pu as well as -0.0227 in Hz, which are far better than the other five models. On the other hand, LQRMFD achieved the lowest ST of 0.55 seconds to mitigate the frequency disturbances, whereas AGC-PID-ANN achieved the second-lowest ST of 0.76 seconds. The rest of the models obtained a slower response to mitigate the frequency disturbances as their obtained STs are relatively higher. Therefore, it can be said that the performance of the LQRMFD model is better than other models in terms of dynamic response parameters, such as, FD and ST.

3.4. Analysis

In case of the proposed model, it is important to know how effective its performance that is compared to the existing models. In this regard, a perfect analysis is required for obtaining the performance improvement of LQRMFD according to (7),

$$\%\, performanceimprovement = \frac{Abs(EP) - Abs(LQRMFD\ Performance)}{Abs(EP)} \times 100 \quad (7)$$

Here, *Abs*(*EP*) refers to the absolute value of existing performances. On the other hand, Abs (LQRMFD performance) signifies the absolute value of the performance of our LQRMFD.

By (7), we calculated the performance improvement in percentages of LQRMFD with self-implemented models as well as existing models of LFC [21], AGC [21], AGC-PID [21], CSU [21], and AGC-PID-ANN [24]. Here, L-LFC, L-AGC, L-AGC-PID refer to LQRMFD with LFC, LQRMFD with AGC, and LQRMFD with AGC-PID, respectively. On the other hand, L-LFC, L-AGC, L-AGC-PID, L-CSU, L-AGC-PID-ANN refer to LQRMFD with LFC [21], LQRMFD with AGC [21], LQRMFD with AGC-PID [21], LQRMFD with CSU [21], LQRMFD with AGC-PID-ANN [24], respectively that are reported in Table 4. In a close look of this table, it is found that our LQRMFD achieved the highest improvement of 96.72% from the LFC-based model in FD in pu, whereas 96.26% improvement was achieved in FD in Hz for the same model. Furthermore, 95% improvement was achieved by LQRMFD from the AGC-based model in ST in mitigating the frequency disturbances. At a glance, in all cases, our LQRMFD achieved a significant improvement compared to the self-implemented other models in terms of dynamic response parameters, such as FD and ST.

In the case of existing models, analytical results exhibited in Table 4 show that our LQRMFD achieved the best improvements of 99.01% and 99.95% in FD in pu and Hz, respectively, for the CSU based model. On the other hand, 94.97% improvement was achieved in ST by LQRMFD from the AGC-based model. However, in all cases, our LQRMFD achieved a significant improvement compared to the existing models in terms of dynamic response parameters, such as, FD and ST.

Table 4. Calculation of performance improvement in percentage for LQRMFD with self-implemented models as well as existing models respectively. Here, "- -" refers to not available

Parameters	Calculation in Percentage							
	L-LFC	L-AGC	L-AGC-PID	L-LFC	L-AGC	L-AGC-PID	L-CSU	L- AGC-PID-ANN
FD $\Delta\Omega$, pu	96.72	95.74	33.33	96.52	94.44	78.95	99.01	- -
FD, $\Delta\Omega$, Hz	96.28	95.16	29.96	96.05	93.70	76.55	99.95	- -
ST, t_s, sec	91.79	95.00	88.29	92.02	94.97	90.60	89.17	27.63

4. CONCLUSION

It is known that an optimal and robust controller is needed to keep the desired frequency in the PS during a CA. In this sense, the existing controllers tried to solve the frequency disturbances during CAs but failed to improve significantly. To overcome the above limitation, LQRMFD incorporates an LQR controller in a PS network during a CA to mitigate the FDs. In arrangement to facilitate such incorporation perfectly, a new PS model has been considered in this paper. Consequently, eliminating the redundancy for PS research as well as diversity can be achieved in such considerations as a common practice exists in the literature of similar PS models in most cases. Thus, to achieve an effective and stable system model in LQRMFD, a new steady-state equation has been derived by solving a new numerical problem. Furthermore, the above combinations ultimately mitigate not only the settlement time but also the FD of the PS during CAs.

In order to obtain the obtained results of our LQRMFD on the particular PS during a CA. Thus, to evaluate the proposed LQRMFD, a series of experiments were carried out in the MATLAB simulator, including the self-implemented system models in terms of FDs and ST. Furthermore, the obtained results of LQRMFD were compared with the results of individual system models with self-implemented models using newly integrated PSs. On the other hand, the results of LQRMFD were also compared with other existing models. In this regard, calculation of performance improvement in percentage for LQRMFD with self-implemented models. Hence, calculation of performance improvement in percentage for LQRMFD with existing models Thus, it can be concluded after observing above-mentioned all the analysis and comparisons that LQRMFD proposed model is better than other controllers in terms of ST and FD in the PS during a CA. In addition, a rigorous analysis of these models was carried out in order to determine the percentage performance improvement of LQRMFD. However, according to detailed comparisons and performance improvement analysis, LQRMFD has a remarkable ability to reduce the FD and ST of the PS during a CA. On the other hand, this controller yielded a much faster response compared to any other controllers in the literature. As a future work, it might be regarded to integrate a stable and reliable control system against illegal approach to cyber security following the self-healing effective process in the proposed LQRMFD. Furthermore, developing a scheme for finding the limitation of the false data injection effect is also left for future tasks.

REFERENCES

[1] R. Nema and A. Trivedi, "Load frequency control of a small isolated power station by using super capacitor based energy storage system," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 1, no. 10, 2012.

[2] Y. Zhang, L. Wang, and W. Sun, "Investigating the impact of cyber attacks on power system reliability," in *2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, May 2013, pp. 462–467, doi: 10.1109/CYBER.2013.6705490.

[3] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *IEEE PES General Meeting*, Jul. 2010, pp. 1–6, doi: 10.1109/PES.2010.5590115.
[4] A. Dagoumas, "Assessing the impact of cybersecurity attacks on power systems," *Energies*, vol. 12, no. 4, Feb. 2019, doi: 10.3390/en12040725.
[5] S. Amin, "For the good of the grid," *IEEE Power and Energy Magazine*, vol. 6, no. 6, pp. 48–59, 2008, doi: 10.1109/MPE.2008.929745.
[6] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012, doi: 10.1109/SURV.2011.122111.00145.
[7] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct. 2010, pp. 244–249, doi: 10.1109/SMARTGRID.2010.5622049.
[8] V. Kučera, "Optimal control: Linear quadratic methods," *Automatica*, vol. 28, no. 5, pp. 1068–1069, Sep. 1992, doi: 10.1016/0005-1098(92)90166-D.
[9] H. Saadat, *Power system analysis*. Mcgraw-Hill, 1999.
[10] H. Bevrani, *Robust power system frequency control*. Boston, MA: Springer US, 2009, doi: 10.1007/978-0-387-84878-5.
[11] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, Apr. 2017, pp. 1–8, doi: 10.1109/CPRE.2017.8090056.
[12] J. Yan, C.-C. Liu, and M. Govindarasu, "Cyber intrusion of wind farm SCADA system and its impact analysis," in *2011 IEEE/PES Power Systems Conference and Exposition*, Mar. 2011, pp. 1–6, doi: 10.1109/PSCE.2011.5772593.
[13] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data Injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, Apr. 2017, doi: 10.1109/TII.2016.2614396.
[14] A. Ginter, "The top 20 cyberattacks on industrial control systems," in *Waterfall Security Solutions Version 1.1*, 2018, pp. 1–28.
[15] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ICS) security," Gaithersburg, MD, Jun. 2015, doi: 10.6028/NIST.SP.800-82r2.
[16] C. Chen, M. Cui, X. Wang, K. Zhang, and S. Yin, "An investigation of coordinated attack on load frequency control," *IEEE Access*, vol. 6, pp. 30414–30423, 2018, doi: 10.1109/ACCESS.2018.2845300.
[17] T. M. Chen, "Stuxnet, the real start of cyber warfare?," *IEEE Network*, vol. 24, no. 6, pp. 2–3, Nov. 2010, doi: 10.1109/MNET.2010.5634434.
[18] R. Tan *et al*., "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017, doi: 10.1109/TIFS.2017.2676721.
[19] S. Biswas and A. Sarwat, "Vulnerabilities in two-area automatic generation control systems under cyberattack," in *2016 Resilience Week (RWS)*, Aug. 2016, pp. 40–45, doi: 10.1109/RWEEK.2016.7573304.
[20] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014, doi: 10.1109/TSG.2014.2298195.
[21] M. A. Rahman, M. S. Rana, and H. R. Pota, "Mitigation of frequency and voltage disruptions in smart grid during cyber-attack," *Journal of Control, Automation and Electrical Systems*, vol. 31, no. 2, pp. 412–421, Apr. 2020, doi: 10.1007/s40313-020-00574-z.
[22] M. I. Mosaad and F. Salem, "LFC based adaptive PID controller using ANN and ANFIS techniques," *Journal of Electrical Systems and Information Technology*, vol. 1, no. 3, pp. 212–222, Dec. 2014, doi: 10.1016/j.jesit.2014.12.004.
[23] M. Hassan, N. K. Roy, and M. Sahabuddin, "Mitigation of frequency disturbance in power systems during cyber-attack," in *2016 2nd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE)*, Dec. 2016, pp. 1–4, doi: 10.1109/ICECTE.2016.7879601.
[24] M. S. Islam, S. Sultana, and M. M. Rahman, "Protection of power system during cyber-attack using artificial neural network," *Engineering International*, vol. 7, no. 2, pp. 73–84, 2019, doi: 10.18034/ei.v7i2.478.
[25] Y. Li, R. Huang, and L. Ma, "False data injection attack and defense method on load frequency control," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2910–2919, Feb. 2021, doi: 10.1109/JIOT.2020.3021429.
[26] M. M. Uddin and M. M. Kabir, "Reduction of frequency disruption during cyber-attack in the power system," in *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, 2020, pp. 1–6, doi: 10.1109/STI50764.2020.9350518.
[27] H. Keshtkar, F. D. Mohammadi, J. Ghorbani, J. Solanki, and A. Feliachi, "Proposing an improved optimal LQR controller for frequency regulation of a smart microgrid in case of cyber intrusions," in *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, May 2014, pp. 1–6, doi: 10.1109/CCECE.2014.6901017.
[28] O. A. Solheim, "Design of optimal control systems with prescribed eigenvalues," *International Journal of Control*, vol. 15, no. 1, pp. 143–160, Jan. 1972, doi: 10.1080/00207177208932136.

BIOGRAPHIES OF AUTHORS

Muhammad Musleh Uddin received an M.Sc. Engineering degree in Electrical and Electronic Engineering (EEE) from the Dhaka University of Engineering and Technology (DUET), Bangladesh. Recently, he joined at Chittagong Institute of Engineering and Technology (CIET), Bangladesh as a principal. He was a research assistant from 2019 to 2020 at the EEE Department of DUET, Bangladesh. His research interests include power system stability, smart grid cybersecurity, and artificial neural networks. He can be contacted by email at muslehduet17@gmail.com.

Kazi Rafiqul Islam received a Ph.D. in the Faculty of Science Engineering and Technology from Swinburne University of Technology, Melbourne, Australia, in 2020. He is an associate professor of the EEE Department at the Dhaka University of Engineering and Technology (DUET), Bangladesh. His major research interest includes power system, biomedical engineering, artificial neural networks, and renewable energy. He has more than ten refereed publications in international journals and conferences. He can be contacted by email at rafiqul@duet.ac.bd.

Md. Monirul Kabir received an M.E. degree in the Department of Human and Artificial Intelligent Systems from the University of Fukui, Japan, in 2008 and a Ph.D. degree in the Department of System Design Engineering from the same university in 2011. He is a professor of the EEE Department at the Dhaka University of Engineering and Technology (DUET), Bangladesh. His major research interest includes power system, IoT, artificial neural networks, evolutionary approaches, and ant colony optimization. He has more than 50 refereed publications in international journals and conferences. He can be contacted by email at munir@duet.ac.bd.